

# A problem of Wang on Davenport constant for the multiplicative semigroup of the quotient ring of $\mathbb{F}_2[x]$

Lizhen Zhang<sup>a,b\*</sup>    Haoli Wang<sup>c†</sup>    Yongke Qu<sup>d‡</sup>

<sup>a</sup>Shanghai Institute of Applied Mathematics and Mechanics

Shanghai University, Shanghai, 200072, P. R. China

<sup>b</sup>Department of Mathematics, Tianjin Polytechnic University, Tianjin, 300387, P. R. China

<sup>c</sup> College of Computer and Information Engineering

Tianjin Normal University, Tianjin, 300387, P. R. China

<sup>d</sup>Department of Mathematics, Luoyang Normal University, Luoyang, 471022, P. R. China

## Abstract

Let  $\mathbb{F}_q[x]$  be the ring of polynomials over the finite field  $\mathbb{F}_q$ , and let  $f$  be a polynomial of  $\mathbb{F}_q[x]$ . Let  $R = \frac{\mathbb{F}_q[x]}{(f)}$  be a quotient ring of  $\mathbb{F}_q[x]$  with  $0 \neq R \neq \mathbb{F}_q[x]$ . Let  $S_R$  be the multiplicative semigroup of the ring  $R$ , and let  $U(S_R)$  be the group of units of  $S_R$ . The Davenport constant  $D(S_R)$  of the multiplicative semigroup  $S_R$  is the least positive integer  $\ell$  such that for any  $\ell$  polynomials  $g_1, g_2, \dots, g_\ell \in \mathbb{F}_q[x]$ , there exists a subset  $I \subseteq [1, \ell]$  with

$$\prod_{i \in I} g_i \equiv \prod_{i=1}^{\ell} g_i \pmod{f}.$$

In this manuscript, we proved that for the case of  $q = 2$ ,

$$D(U(S_R)) \leq D(S_R) \leq D(U(S_R)) + \delta_f,$$

---

\*Email: lzhzhang0@aliyun.com

†Corresponding author's Email: bjpeuwanghaoli@163.com

‡Email: yongke1239@163.com

where

$$\delta_f = \begin{cases} 0 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) = 1_{\mathbb{F}_2} \\ 1 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) \in \{x, x + 1_{\mathbb{F}_2}\} \\ 2 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) = x * (x + 1_{\mathbb{F}_2}) \end{cases}$$

which partially answered an open problem of Wang on Davenport constant for the multiplicative semigroup of  $\frac{\mathbb{F}_q[x]}{(f)}$  (G.Q. Wang, *Davenport constant for semigroups II*, Journal of Number Theory, 155 (2015) 124–134).

**Key Words:** Zero-sum; Davenport constant; Multiplicative semigroups; Polynomial rings

## 1 Introduction

The additive properties of sequences in abelian groups have been widely studied in the field of Zero-sum Theory (see [3] for a survey), since H. Davenport [2] in 1966 and K. Rogers [5] in 1963 independently proposed one combinatorial invariant, denoted  $D(G)$ , for any finite abelian group  $G$ , which is defined as the smallest  $\ell \in \mathbb{N}$  such that every sequence  $T$  of terms from the group  $G$  of length at least  $\ell$  contains a nonempty subsequence  $T'$  with sum of all terms from  $T'$  being equal to the identity element of the group  $G$ . The Davenport constant is a central concept of zero-sum theory and has been investigated by many researchers in the scope of finite abelian groups.

In 2008, Gao and Wang [9] formulated the definition of Davenport constant for commutative semigroups, and made several related additive researches (see [1, 6–8]).

**Definition A.** [9] *Let  $S$  be a commutative semigroup (not necessary finite). Let  $T$  be a sequence of terms from the semigroup  $S$ . We call  $T$  reducible if  $T$  contains a proper subsequence  $T'$  ( $T' \neq T$ ) such that the sum of all terms of  $T'$  equals the sum of all terms of  $T$ . Define the Davenport constant of the semigroup  $S$ , denoted  $D(S)$ , to be the smallest  $\ell \in \mathbb{N} \cup \{\infty\}$  such that every sequence  $T$  of length at least  $\ell$  of terms from  $S$  is reducible.*

Before then, starting from the research of Factorization Theory in Algebra, A. Geroldinger and F. Halter-Koch in 2006 have formulated another closely related definition,  $d(S)$ , for any commutative semigroup  $S$ , which is called the small Davenport constant.

**Definition B.** (Definition 2.8.12 in [4]) *For a commutative semigroup  $S$ , let  $d(S)$  denote the smallest  $\ell \in \mathbb{N}_0 \cup \{\infty\}$  with the following property:*

For any  $m \in \mathbb{N}$  and  $a_1, \dots, a_m \in \mathcal{S}$  there exists a subset  $I \subset [1, m]$  such that  $|I| \leq \ell$  and

$$\sum_{i=1}^m a_i = \sum_{i \in I} a_i.$$

The following connection between the (large) Davenport constant  $D(\mathcal{S})$  and the small Davenport constant  $d(\mathcal{S})$  was also obtained for any commutative semigroup  $\mathcal{S}$ .

**Proposition C.** ([7]) *Let  $\mathcal{S}$  be a commutative semigroup. Then  $D(\mathcal{S})$  is finite if and only if  $d(\mathcal{S})$  is finite. Moreover, in case that  $D(\mathcal{S})$  is finite, we have*

$$D(\mathcal{S}) = d(\mathcal{S}) + 1.$$

Very recently, Wang in 2015 obtained the following result on Davenport constant for the multiplicative semigroup associated with polynomial rings  $\mathbb{F}_q[x]$ .

**Proposition D.** ([6]) *Let  $q > 2$  be a prime power, and let  $\mathbb{F}_q[x]$  be the ring of polynomials over the finite field  $\mathbb{F}_q$ . Let  $R$  be a quotient ring of  $\mathbb{F}_q[x]$  with  $0 \neq R \neq \mathbb{F}_q[x]$ . Then*

$$D(\mathcal{S}_R) = D(\mathcal{U}(\mathcal{S}_R)),$$

where  $\mathcal{S}_R$  denotes the multiplicative semigroup of the ring  $R$ , and  $\mathcal{U}(\mathcal{S}_R)$  denotes the group of units in  $\mathcal{S}_R$ .

However, for the case of  $q = 2$ , Wang proposed it as an open problem.

**Problem E.** (see concluding remarks in [6]) *Let  $R$  be a quotient ring of  $\mathbb{F}_2[x]$  with  $0 \neq R \neq \mathbb{F}_2[x]$ . Determine  $D(\mathcal{S}_R) - D(\mathcal{U}(\mathcal{S}_R))$ .*

In this manuscript, we considered this open problem. By using the method employed by Wang, we obtained the following result, which is a partial solution of Problem E.

**Theorem 1.1.** *Let  $\mathbb{F}_2[x]$  be the ring of polynomials over the finite field  $\mathbb{F}_2$ , and let  $R = \frac{\mathbb{F}_2[x]}{(f)}$  be a quotient ring of  $\mathbb{F}_2[x]$  where  $f \in \mathbb{F}_2[x]$  and  $0 \neq R \neq \mathbb{F}_2[x]$ . Then*

$$D(\mathcal{U}(\mathcal{S}_R)) \leq D(\mathcal{S}_R) \leq D(\mathcal{U}(\mathcal{S}_R)) + \delta_f,$$

where

$$\delta_f = \begin{cases} 0 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) = 1_{\mathbb{F}_2}; \\ 1 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) \in \{x, x + 1_{\mathbb{F}_2}\}; \\ 2 & \text{if } \gcd(x * (x + 1_{\mathbb{F}_2}), f) = x * (x + 1_{\mathbb{F}_2}). \end{cases}$$

## 2 The proof of Theorem 1.1

The notations and terminologies used here are consistent to ones used in [1, 6–8]. For the reader's convenience, we need to give some necessary ones.

Let  $\mathcal{S}$  be a finite commutative semigroup. The operation on  $\mathcal{S}$  is denoted by  $+$ . The identity element of  $\mathcal{S}$ , denoted  $0_{\mathcal{S}}$  (if exists), is the unique element  $e$  of  $\mathcal{S}$  such that  $e + a = a$  for every  $a \in \mathcal{S}$ . If  $\mathcal{S}$  has an identity element  $0_{\mathcal{S}}$ , let

$$U(\mathcal{S}) = \{a \in \mathcal{S} : a + a' = 0_{\mathcal{S}} \text{ for some } a' \in \mathcal{S}\}$$

be the group of units of  $\mathcal{S}$ . For any element  $c \in \mathcal{S}$ , let

$$\text{St}(c) = \{a \in U(\mathcal{S}) : a + c = c\}$$

denote the stabilizer of  $c$  in the group  $U(\mathcal{S})$ . The Green's preorder of the semigroup  $\mathcal{S}$ , denoted  $\leq_{\mathcal{H}}$ , is defined by

$$a \leq_{\mathcal{H}} b \Leftrightarrow a = b \text{ or } a = b + c$$

for some  $c \in \mathcal{S}$ . The Green's congruence of  $\mathcal{S}$ , denoted  $\mathcal{H}$ , is defined by:

$$a \mathcal{H} b \Leftrightarrow a \leq_{\mathcal{H}} b \text{ and } b \leq_{\mathcal{H}} a.$$

We write  $a <_{\mathcal{H}} b$  to mean that  $a \leq_{\mathcal{H}} b$  but  $a \mathcal{H} b$  does not hold.

The sequence  $T$  of terms from the semigroups  $\mathcal{S}$  is denoted by

$$T = a_1 a_2 \cdot \dots \cdot a_{\ell} = \prod_{a \in \mathcal{S}} a^{[v_a(T)]},$$

where  $[v_a(T)]$  means that the element  $a$  occurs  $v_a(T)$  times in the sequence  $T$ . By  $\cdot$  we denote the operation to join sequences. By  $|T|$  we denote the length of the sequence, i.e.,

$$|T| = \sum_{a \in \mathcal{S}} v_a(T) = \ell.$$

Let  $T_1, T_2$  be two sequences of terms from the semigroups  $\mathcal{S}$ . We call  $T_2$  a subsequence of  $T_1$  if

$$v_a(T_2) \leq v_a(T_1)$$

for every element  $a \in \mathcal{S}$ , denoted by

$$T_2 \mid T_1.$$

In particular, if  $T_2 \neq T_1$ , we call  $T_2$  a *proper* subsequence of  $T_1$ , and write

$$T_3 = T_1 T_2^{[-1]}$$

to mean the unique subsequence of  $T_1$  with  $T_2 \cdot T_3 = T_1$ . Let

$$\sigma(T) = a_1 + a_2 + \cdots + a_\ell$$

be the sum of all terms of the sequence  $T$ . By  $\varepsilon$  we denote the empty sequence. If  $S$  has an identity element  $0_S$ , we allow  $T = \varepsilon$  and adopt the convention that  $\sigma(\varepsilon) = 0_S$ . We say that  $T$  is *reducible* if  $\sigma(T') = \sigma(T)$  for some proper subsequence  $T'$  of  $T$  (note that,  $T'$  is probably the empty sequence  $\varepsilon$  if  $S$  has the identity element  $0_S$  and  $\sigma(T) = 0_S$ ). Otherwise, we call  $T$  *irreducible*.

Throughout this paper, we shall always denote

$$R = \mathbb{F}_2[x] / (f)$$

to be the quotient ring of  $\mathbb{F}_2[x]$  modulo some nonconstant polynomial  $f \in \mathbb{F}_2[x]$ , where

$$f = f_1^{n_1} * f_2^{n_2} * \cdots * f_r^{n_r}, \quad (1)$$

such that  $f_1, f_2, \dots, f_r$  are pairwise non-associate irreducible polynomials of  $\mathbb{F}_2[x]$  with

$$f_1 = x, \quad f_2 = x + 1_{\mathbb{F}_2},$$

$$n_1 \geq 0, n_2 \geq 0, n_3, n_4, \dots, n_r \geq 1.$$

Let  $\mathcal{S}_R$  be the multiplicative semigroup of the ring  $R$ . For any element  $a \in \mathcal{S}_R$ , let  $\theta_a \in \mathbb{F}_2[x]$  be the unique polynomial corresponding to the element  $a$  with the least degree, i.e.,

$$\overline{\theta_a} = \theta_a + (f)$$

is the corresponding form of  $a$  in the quotient ring  $R$  with

$$\deg(\theta_a) \leq \deg(f) - 1.$$

By  $\gcd(\theta_a, f)$  we denote the greatest common divisor of the two polynomials  $\theta_a$  and  $f$  in  $\mathbb{F}_2[x]$  (the unique polynomial with the greatest degree which divides both  $\theta_a$  and  $f$ ), in particular, by (1), we have

$$\gcd(\theta_a, f) = f_1^{\alpha_1} * f_2^{\alpha_2} * \cdots * f_r^{\alpha_r} \quad (2)$$

where  $\alpha_i \in [0, n_i]$  for each  $i \in [1, r]$ .

For any polynomial  $g$  and any irreducible polynomial  $h$  of  $\mathbb{F}_2[x]$ , let  $\text{pot}_h(g)$  be the largest integer  $k$  such that  $h^k \mid g$ . Then in (2),  $\alpha_i = \text{pot}_{f_i}(\gcd(\theta_a, f))$  for each  $i \in [1, r]$ . It is easy to observe that for any two element  $a, b \in \mathcal{S}_R$ ,

$$\gcd(\theta_a, f) = \gcd(\theta_b, f)$$

if and only if

$$\text{pot}_{f_i}(\gcd(\theta_a, f)) = \text{pot}_{f_i}(\gcd(\theta_b, f)) \text{ for each } i \in [1, r].$$

To prove Theorem 1.1, we still need some lemmas.

**Lemma 2.1.** ([4], Lemma 6.1.3) *Let  $G$  be a finite abelian group, and let  $H$  be a subgroup of  $G$ . Then,  $D(G) \geq D(G/H) + D(H) - 1$ .*

**Lemma 2.2.** (see [9], Proposition 1.2) *Let  $\mathcal{S}$  be a finite commutative semigroup with an identity. Then  $D(U(\mathcal{S})) \leq D(\mathcal{S})$ .*

**Lemma 2.3.** *Let  $a$  and  $b$  be two elements of  $\mathcal{S}_R$  with  $a \leq_{\mathcal{H}} b$ . Let  $\alpha_i = \text{pot}_{f_i}(\gcd(\theta_a, f))$  and  $\beta_i = \text{pot}_{f_i}(\gcd(\theta_b, f))$  for each  $i \in [1, r]$ . Then,*

(i).  $\text{St}(b) \subseteq \text{St}(a)$  and  $\beta_i \leq \alpha_i$  for each  $i \in [1, r]$ , in particular, if  $a \mathcal{H} b$  then  $\text{St}(b) = \text{St}(a)$  and  $\beta_i = \alpha_i$  for each  $i \in [1, r]$ ;

(ii). if  $\beta_i = \alpha_i$  for each  $i \in [1, r]$ , then  $a \mathcal{H} b$ ;

(iii). If  $a <_{\mathcal{H}} b$  and  $(\alpha_1 - \beta_1)(2n_1 - 1 - \alpha_1 - \beta_1) + (\alpha_2 - \beta_2)(2n_2 - 1 - \alpha_2 - \beta_2) + \sum_{i=3}^r (\alpha_i - \beta_i) > 0$ , then  $\text{St}(b) \subsetneq \text{St}(a)$ .

*Proof of Lemma 2.3.* Note first that  $a \leq_{\mathcal{H}} b$  implies that

$$\alpha_i \geq \beta_i \text{ for each } i \in [1, r].$$

(i). Since  $\mathcal{S}_R$  has the identity element  $0_{\mathcal{S}_R}$ , it follows from  $a \leq_{\mathcal{H}} b$  that

$$a = b + c \text{ for some } c \in \mathcal{S}_R.$$

It follows that

$$\gcd(\theta_b, f) \mid \gcd(\theta_b * \theta_c, f) = \gcd(\theta_a, f),$$

equivalently,  $\beta_i \leq \alpha_i$  for each  $i \in [1, r]$ .

Take an arbitrary element  $d \in \text{St}(b)$ . Then  $d + a = d + (b + c) = (d + b) + c = b + c = a$ , and so  $d \in \text{St}(a)$ . It follows that

$$\text{St}(b) \subseteq \text{St}(a).$$

If  $a \mathcal{H} b$ , i.e.,  $a \leq_{\mathcal{H}} b$  and  $b \leq_{\mathcal{H}} a$ , then  $\text{St}(b) = \text{St}(a)$  and  $\beta_i = \alpha_i$  for each  $i \in [1, r]$  follows readily. This proves Conclusion (i).

(ii). Assume  $\beta_i = \alpha_i$  for each  $i \in [1, r]$ , that is,

$$\gcd(\theta_b, f) = \gcd(\theta_a, f).$$

It follows that there exist polynomials  $h, h' \in \mathbb{F}_q[x]$  such that

$$\theta_a * h \equiv \theta_b \pmod{f}$$

and

$$\theta_b * h' \equiv \theta_a \pmod{f}.$$

It follows that  $b \leq_{\mathcal{H}} a$  and  $a \leq_{\mathcal{H}} b$ , i.e.,

$$a \mathcal{H} b,$$

and Conclusion (ii) is proved.

(iii). Now assume

$$a <_{\mathcal{H}} b$$

and

$$\sum_{i=3}^r (\alpha_i - \beta_i) + (\alpha_1 - \beta_1)(2n_1 - 1 - \alpha_1 - \beta_1) + (\alpha_2 - \beta_2)(2n_2 - 1 - \alpha_2 - \beta_2) > 0. \quad (3)$$

It is sufficient to find some element  $d \in \text{U}(\mathcal{S}_R)$  such that  $d \in \text{St}(a) \setminus \text{St}(b)$ . We shall distinguish two cases.

**Case 1.**  $\sum_{i=3}^r (\alpha_i - \beta_i) > 0$ .

Then there exists some  $i \in [3, r]$  such that  $\alpha_i > \beta_i$ , say

$$\alpha_3 > \beta_3. \quad (4)$$

Take an polynomial

$$h = \frac{f}{f_3^{\alpha_3}}. \quad (5)$$

We show that

$$\gcd(h + 1_{\mathbb{F}_2}, f) = 1_{\mathbb{F}_2} \quad (6)$$

or

$$\gcd(x * h + 1_{\mathbb{F}_2}, f) = 1_{\mathbb{F}_2}. \quad (7)$$

Suppose to the contrary that  $\gcd(h + 1_{\mathbb{F}_2}, f) \neq 1_{\mathbb{F}_2}$  and  $\gcd(x * h + 1_{\mathbb{F}_2}, f) \neq 1_{\mathbb{F}_2}$ . By (1) and (5), we have that  $f_i \nmid \gcd(h + 1_{\mathbb{F}_2}, f)$  and  $f_i \nmid \gcd(x * h + 1_{\mathbb{F}_2}, f)$  for each  $i \in [1, r] \setminus \{3\}$ . This implies that  $f_3 \mid (h + 1_{\mathbb{F}_2})$  and  $f_3 \mid (x * h + 1_{\mathbb{F}_2})$ , and thus,  $f_3 \mid x * (h + 1_{\mathbb{F}_2}) - (x * h + 1_{\mathbb{F}_2}) = x + 1_{\mathbb{F}_2}$ , which is absurd. This proves that (6) or (7) holds.

Take an element  $d \in \mathcal{S}_R$  with

$$\theta_d \equiv h + 1_{\mathbb{F}_2} \pmod{f}$$

or

$$\theta_d \equiv x * h + 1_{\mathbb{F}_2} \pmod{f}$$

according to (6) or (7) holds respectively. It follows that

$$d \in \mathcal{U}(\mathcal{S}_R),$$

and follows from (4) and (5) that

$$\theta_a * \theta_d \equiv \theta_a \pmod{f}$$

and

$$\theta_b * \theta_d \not\equiv \theta_b \pmod{f}.$$

That is,  $d \in \text{St}(a) \setminus \text{St}(b)$ , which implies

$$\text{St}(b) \subsetneq \text{St}(a).$$

**Case 2.**  $(\alpha_1 - \beta_1)(2n_1 - 1 - \alpha_1 - \beta_1) > 0$  or  $(\alpha_2 - \beta_2)(2n_2 - 1 - \alpha_2 - \beta_2) > 0$ .

Say

$$(\alpha_1 - \beta_1)(2n_1 - 1 - \alpha_1 - \beta_1) > 0.$$

It follows that

$$\alpha_1 > \beta_1 \quad (8)$$

and

$$n_1 > \beta_1 + 1. \quad (9)$$



Take an polynomial

$$h = \frac{f}{f_1^{\beta_1+1}}. \quad (10)$$

Combined with (9) and (10), we conclude that

$$\gcd(h + 1_{\mathbb{F}_2}, f) = 1_{\mathbb{F}_2}.$$

Take an element  $d \in \mathcal{S}_R$  with

$$\theta_d \equiv h + 1_{\mathbb{F}_2} \pmod{f}.$$

It follows that

$$d \in \mathbf{U}(\mathcal{S}_R),$$

and follows from (8) and (10) that

$$\theta_a * \theta_d \equiv \theta_a \pmod{f}$$

and

$$\theta_b * \theta_d \not\equiv \theta_b \pmod{f}.$$

That is,  $d \in \text{St}(a) \setminus \text{St}(b)$  which implies

$$\text{St}(b) \subsetneq \text{St}(a).$$

This proves Lemma 2.3. □

Now we are in a position to prove Theorem 1.1.

*Proof of Theorem 1.1.* By Lemma 2.2, it suffices to show that  $\mathbf{D}(\mathcal{S}_R) \leq \mathbf{D}(\mathbf{U}(\mathcal{S}_R)) + \delta_f$ . Let  $T = a_1 a_2 \cdots a_\ell$  be an arbitrary sequence of terms from  $\mathcal{S}_R$  of length

$$\ell = \mathbf{D}(\mathbf{U}(\mathcal{S}_R)) + \delta_f. \quad (11)$$

We shall prove that  $T$  contains a *proper* subsequence  $T'$  with  $\sigma(T') = \sigma(T)$ .

Take a shortest subsequence  $V$  of  $T$  such that

$$\sigma(V) \mathcal{H} \sigma(T). \quad (12)$$

We may assume without loss of generality that

$$V = a_1 \cdot a_2 \cdots a_t \quad \text{where } t \in [0, \ell].$$

By the minimality of  $|V|$ , we derive that

$$0_{S_R} >_{\mathcal{H}} a_1 >_{\mathcal{H}} (a_1 + a_2) >_{\mathcal{H}} \cdots >_{\mathcal{H}} \sum_{i=1}^t a_i.$$

Denote

$$K_0 = \{0_{S_R}\}$$

and

$$K_i = \text{St}\left(\sum_{j=1}^i a_j\right) \text{ for each } i \in [1, t].$$

Note that  $K_i$  is a subgroup of  $U(S_R)$  for each  $i \in [1, t]$ . Moreover, since  $\text{St}(0_{S_R}) = K_0$ , it follows from Conclusion (i) of Lemma 2.3 that

$$K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_t,$$

and moreover, by applying Lemma 2.3, we conclude that there exists a subset  $M$  of  $[0, t-1]$  with

$$|M| \geq t - \delta_f \tag{13}$$

such that

$$K_i \subsetneq K_{i+1} \text{ for each } i \in M.$$

For  $i \in M$ , since  $\frac{U(S_R)}{K_{i+1}} \cong \frac{U(S_R)/K_i}{K_{i+1}/K_i}$  and  $D(K_{i+1}/K_i) \geq 2$ , it follows from Lemma 2.1 that

$$\begin{aligned} D(U(S_R)/K_{i+1}) &= D\left(\frac{U(S_R)/K_i}{K_{i+1}/K_i}\right) \\ &\leq D(U(S_R)/K_i) - (D(K_{i+1}/K_i) - 1) \\ &\leq D(U(S_R)/K_i) - 1. \end{aligned} \tag{14}$$

Combined with (11), (13) and (14), we conclude that

$$\begin{aligned} 1 \leq D(U(S_R)/K_t) &\leq D(U(S_R)/K_0) - |M| \\ &\leq D(U(S_R)) - (t - \delta_f) \\ &= (\ell - \delta_f) - (t - \delta_f) \\ &= \ell - t \\ &= |TV^{[-1]}|. \end{aligned} \tag{15}$$

By Conclusion (i) of Lemma 2.3 and (12), we have

$$\text{pot}_{f_i}(\gcd(\theta_{\sigma(V)}, f)) = \text{pot}_{f_i}(\gcd(\theta_{\sigma(T)}, f)) \tag{16}$$

for each  $i \in [1, r]$ . Let

$$\mathcal{J} = \{j \in [1, r] : f_j^{n_j} \mid \theta_{\sigma(T)}\}.$$

By (16), we have that

$$f_i \nmid \theta_a \text{ for each term } a \text{ of } TV^{[-1]} \text{ and each } i \in [1, r] \setminus \mathcal{J}, \quad (17)$$

and that

$$f_j^{n_j} \mid \theta_{\sigma(V)} \text{ for each } j \in \mathcal{J}. \quad (18)$$

For each term  $a$  of  $TV^{[-1]}$ , let  $\tilde{a}$  be the element of  $\mathcal{S}_R$  such that

$$\theta_{\tilde{a}} \equiv \theta_a \pmod{f_i^{n_i}} \text{ for each } i \in [1, r] \setminus \mathcal{J} \quad (19)$$

and

$$\theta_{\tilde{a}} \equiv 1_{\mathbb{F}_2} \pmod{f_j^{n_j}} \text{ for each } j \in \mathcal{J}. \quad (20)$$

By (17), (19) and (20), we conclude that  $\gcd(\theta_{\tilde{a}}, f) = 1_{\mathbb{F}_2}$ , i.e.,

$$\tilde{a} \in U(\mathcal{S}_R) \text{ for each term } a \text{ of } TV^{[-1]}. \quad (21)$$

By (18) and (19), we conclude that

$$\sigma(V) + \tilde{a} = \sigma(V) + a \text{ for each term } a \text{ of } TV^{[-1]}. \quad (22)$$

By (15) and (21), we have that  $\coprod_{a \in TV^{[-1]}} \tilde{a}$  is a nonempty sequence of elements in  $U(\mathcal{S}_R)$  of length  $|\coprod_{a \in TV^{[-1]}} \tilde{a}| = |TV^{[-1]}| \geq D(U(\mathcal{S}_R)/K_t)$ . It follows that there exists a **nonempty** subsequence

$$W \mid TV^{[-1]}$$

such that

$$\sigma\left(\coprod_{a \in W} \tilde{a}\right) \in K_t$$

which implies

$$\sigma(V) + \sigma\left(\coprod_{a \in W} \tilde{a}\right) = \sigma(V). \quad (23)$$

By (22) and (23), we conclude that

$$\begin{aligned} \sigma(T) &= \sigma(TW^{[-1]}V^{[-1]}) + (\sigma(V) + \sigma(W)) \\ &= \sigma(TW^{[-1]}V^{[-1]}) + (\sigma(V) + \sigma(\coprod_{a \in W} \tilde{a})) \\ &= \sigma(TW^{[-1]}V^{[-1]}) + \sigma(V) \\ &= \sigma(TW^{[-1]}), \end{aligned}$$

and  $T' = TW^{[-1]}$  is the desired proper subsequence of  $T$ . This completes the proof of the theorem.  $\square$

## Acknowledgements

This work is supported by NSFC (11301381, 11172158, 61303023, 11371184, 11426128), Science and Technology Development Fund of Tianjin Higher Institutions (20121003), Doctoral Fund of Tianjin Normal University (52XB1202).

## References

- [1] S.D. Adhikari, W.D. Gao and G.Q. Wang, *Erdős-Ginzburg-Ziv theorem for finite commutative semigroups*, Semigroup Forum, **88** (2014) 555–568.
- [2] H. Davenport, Proceedings of the Midwestern conference on group theory and number theory, Ohio State University, April 1966.
- [3] W.D. Gao and A. Geroldinger, *Zero-sum problems in finite abelian groups: a survey*, Expo. Math., **24** (2006) 337–369.
- [4] A. Geroldinger and F. Halter-Koch, *Non-Unique Factorizations. Algebraic, Combinatorial and Analytic Theory*, Pure and Applied Mathematics, vol. 278, Chapman & Hall/CRC, 2006.
- [5] K. Rogers, *A Combinatorial problem in Abelian groups*, Proc. Cambridge Phil. Soc., **59** (1963) 559–562.
- [6] G.Q. Wang, *Davenport constant for semigroups II*, Journal of Number Theory, **155** (2015) 124–134.
- [7] G.Q. Wang, *Additively irreducible sequences in commutative semigroups*, arXiv:1504.06818.
- [8] G.Q. Wang, *Structure of the largest idempotent-free sequences in finite semigroups*, arXiv:1405.6278.
- [9] G.Q. Wang and W.D. Gao, *Davenport constant for semigroups*, Semigroup Forum, **76** (2008) 234–238.